State of Arizona

Department of Economic Security Information Technology Standards	Title: 1-38-0076 DES Account Management Procedures	
Subject: This procedure outlines the computer account management process at DES.	***Effective Date:*** 03/07/05	***Revision:*** 1.1

1. **Summary of Procedure Changes**

   1.1. 09/30/05 – Minor changes by ITSA.

2. **Purpose**

   The purpose of this procedure is to outline the computer account management process at DES. These rules are in place to protect the employee, the agency, and the agency's physical and virtual assets. If these procedures are not followed, inappropriate access may be applied which can lead to compromise of the Confidentiality, Integrity and Availability of Department data.

3. **Scope**

   This procedure applies to employees, contractors, consultants, temporaries, and other workers at DES. It applies to all equipment that is owned or leased by DES. Furthermore, it applies to any account that is needed to access any desktop or server on the DES network.

   The targeted audience for this document is: Division and Program Security Analysts, LAN Teams, the Resolution Center, Managers and Supervisors within DES.

4. **Responsibilities**

   4.1. The DES Director, Deputy Directors, Associate Director, and Assistant Directors are responsible for implementing and enforcing this procedure.

   4.2. The DES CIO and the DES Division of Technology Services is responsible for implementing this procedure.

   4.3. DES divisions and programs are responsible for implementing this procedure and monitoring compliance for the users and systems that they implement or sponsor.

5. **Definitions and Abbreviations**

   5.1. **Abbreviations**

   5.1.1. **AHCCCS** – **A**rizona **H**ealth **C**are **C**ost **C**ontainment **S**ystem

   5.1.2. **CIO** – **C**hief **I**nformation **O**fficer

   5.1.3. **CISO –** **C**hief **I**nformation **S**ecurity **O**fficer

   5.1.4. **DTS** – **D**ivision of **T**echnology **S**ervices

   5.1.5. **DES** – **D**epartment of **E**conomic **S**ecurity

   5.1.6. **GITA** – **G**overnment **I**nformation **T**echnology **A**gency

   5.1.7. **IT** – **I**nformation **T**echnology

   5.1.8. **ISA** – **I**nformation **S**ecurity **A**dministration

6. **Procedure**

   Note: All forms mentioned in this document can be found either on the DES Intranet or Outlook Public Folders.

6.1. New Employee Accounts

6.1.1 The hiring manager/supervisor must complete a J125 form for internal employees and forward to the security analyst for their Division or Program to open new accounts.

6.1.2. All new computer accounts will be requested as soon as possible (a minimum of two weeks) prior to employee start date.

6.1.3. Online or hardcopy forms will be accepted.

6.1.4. Any access that the employee will need must be indicated on the form at the time the new account is requested.

6.1.5. The completed forms that are received by the security analyst will be retained for the time that the employee is employed by DES. Any updates of access made must be kept with the original form to track the authorization levels of the accounts.

6.1.6. All new employees must read the Security Awareness Training Manual and sign a J129 User Affirmation Statement as well.

6.2. Updated Employee Access

If an employee remains in the same job but requires updated access (additional or removal), the procedure for new accounts can be followed, with the exception that the J125 indicate that this is an existing employee. All access change requests must be kept with the original form for tracking purposes.

6.3. Transfer Employee Accounts

6.3.1. It is the responsibility of both the transferee’s new and prior supervisor or manager to ensure that the new access that is required is added, as well as the old access is removed. This must be done via the J125 form (online or hard copy).

6.3.2. The prior supervisor or manager must submit a form requesting the prior access be removed.

6.3.3. The new supervisor or manager must submit a form requesting the new access be granted.

6.3.4. The forms that are received by the security analyst will be retained for the time that the employee is employed by DES. Any updates of access made must be kept with the original form to track the authorization levels of the accounts.

6.3.5. The Division where the employee has departed from will own the employee’s data.

6.4. Terminated Employee Accounts

6.4.1. All DES users must be deleted from both the DES and non-DES computer systems as soon as possible after the date of resignation or termination (refer to deletion process below). It is the responsibility of Management to complete the Request for Terminal Access and Other Activities, form J-125 (remove all access), as part of the employee termination process. Management will then forward the J-125 (electronic or hard copy) to the Division or Program Security Office. The Security Analyst will perform the deletion process or send to CSSC, if appropriate.

6.4.2. If the DES terminated user had access to the AHCCCS computer system, the DOA computer system and/or the ADOT/MVD computer system, management must forward additional access forms for deletion from those computer systems. The AHCCCS form is User Access Request Form MD2800, the DOA form is Request for Data System Access, and the ADOT/MVD form is Computer Access Request. These request forms for deletion must be forwarded to the Division or Program Security Office where the Security Analyst will perform the deletion process.

6.4.3. Non-DES terminated users must be deleted from the DES computer systems as soon as possible after the date of resignation or termination. Each non-DES entity with access to DES computer systems completed and signed a Data Sharing Request/Agreement. That agreement stipulates that a Request for Terminal Access and Other Activities, form J-125 will be forwarded to the DES ISA upon the termination of a user. The Security Analyst at the ISA will perform the deletion process or send to the appropriate entity.

6.4.4. Upon receipt of the J-125, the terminated user's OUTLOOK mailbox content will be archived and stored on the SAN for one year. If a program has retention requirements beyond this period management should note the requirement on the J-125. It is the local Exchange Administrator's responsibility to perform the archive, storage, and removal after the retention period has lapsed.

6.4.5. The terminated user's data files will be stored on the SAN for a period of one year. If the program has retention requirements beyond this period, management should note the length of retention on the J-125. It is the local LAN support staff responsibility to coordinate the retention of the files and delete the data after the retention period has lapsed.

6.5. Procedure Contingency

6.5.1. When Management fails to provide the necessary paperwork to remove a user from the computer systems and it is known that the user has terminated, the Division or Program Security Analyst will continue to request the correct paperwork from Management but must also put the user account(s) in a non access condition. When the deletion documents are still not provided, the Division or Program Security Analyst will have to take the initiative and not only perform the deletion process but also prepare the deletion paperwork for documentation purposes.

6.5.2. Security Analysts have a wide range of available options. They can prepare a J-125 in the same manner as management, they can use the original add access J-125 and indicate it is the deletion document, they can prepare a form of correspondence that includes the user's name, logonid, OpId and user identification code and forward any of these alternatives as outlined in the Deletion Process for DES Users.

6.6. Emergency Termination

An emergency termination requires immediate action. Management must inform the Division or Program Security Office of the current or pending action and the Security Analyst will put the user accounts in a non-access condition based on the information supplied. This action can be initiated by management with a phone call, an e-mail message, a visit, or any form of official correspondence. Management must also provide the correct deletion paperwork as soon as possible for the deletion process to occur.

6.7. Deletion Process for DES Users

The deletion process requires removal from LANs, WANs, network applications, internet, extranet, intranet, e-mail, mainframe, division and program applications, data set access permissions, SYSM, NATURAL, and other previously granted access.

6.7.1. Management staff prepares a form J-125 with “remove all access” indicated. This form is sent to the Division or Program Security Office,

6.7.2. The Security Analyst processes the form by supplying user access information and listing applications, data sets, libraries, remote access tools and/or SecurId cards/FOBs, etc. that were previously granted and not indicated on the form,

6.7.3. The Security Analyst removes access to information under the control of the user’s immediate division or program,

6.7.4. The Security Analyst forwards the form to all Division and Program Security Offices who supplied the user with access to their information,

6.7.5. The Security Analyst forwards the form to all respective WAN and LAN administrators,

6.7.6. The Security Analyst forwards the form to the DES Warehouse security staff,

6.7.7. The Security Analyst forwards the form to the CSSC,

6.7.8. The Security Analyst forwards the form to DSS,

6.7.9. The Security Analyst forwards all ADOT/Motor Vehicle Division and AHCCCS deletion forms to the Information Security Administration. ADOA deletion forms are either forwarded to the Information Security Administration or the Division of Business and Finance depending on the application involved.

6.7.10. The Security Analyst files all J-125s and the J-129 “User Affirmation Statement” in the deletion file and/or folder.

6.7.11. The Exchange Administrator will create PST files of the mailbox contents and store the archive on the SAN for a period of one year (unless otherwise noted on the J-125).

6.7.12. The Exchange Administrator will terminate the account, stop incoming and outgoing mail, hide the account in the Global Catalogue and remove the account from Distribution Lists.

6.7.13. After 30 days, the account will be deleted.

6.7.14. The Exchange Administrator will remove the PST files after the specified retention period lapses (one year is standard).

6.7.15. The Local Area Network Administrator will coordinate the archive of the terminated user’s data files (Home Directory contents) on the SAN.

6.7.16. The Local Area Network Administrator will remove the archived files after the specified retention period (one year is standard).

6.7.17. The Division where the employee has departed from will own the employee’s data.

6.8. Deletion Process for non-DES Users

All deletion activity will be processed through the Information Security Administration or selected DES Divisions who process providers and contractors. The process is the same as the termination process.

6.9. Reports (Non-Use & Termination)

Each month a report is distributed showing all users who have not accessed the DES mainframe for the past 30 days. All user accounts on this report shall be placed in suspend (non-access condition). Management should be notified of the condition and told of the need for deletion paperwork if that is the case. If other conditions are causing the non-use, that can be documented in the user's access file and coded in the logonid record as determined by the division or program security staff.

Each month a report is distributed showing all users who have not accessed the DES mainframe for the past 90 days. Again , management should be notified of the condition and told to supply the necessary deletion paperwork if the user has terminated. If other conditions are causing the non-use, that can be documented in the user's access file and coded in the logonid record as determined by the division or program security staff. If paperwork is not provided by management, the Security Analyst will have to defer to the Procedure Contingency section.

6.10. Non-DES Employees

6.10.1. All new computer accounts will be requested as soon as possible (a minimum of at least two weeks) prior to contractor start date through the J125 form.

6.10.2. A defined time period for the term of the contract must be given at the time of the account request. After this time, the contractor's account will be expired unless manager approval has been received by the appropriate account manager for an extension of a specified time.

6.10.3. For terminated contractors, a J125 form must be submitted (via electronic or hard copy) as soon as the contractor no longer needs access to the DES network. This is the responsibility of the direct supervisor of the contractor or the manager of the division or program for which they worked.

6.11. Requests for System/Generic Accounts

6.11.1 Requests for system/generic accounts must be accompanied by a justification authored by the requestor and signed off by their manager.

6.11.2. The Chief Information Security Officer must approve all system and generic accounts.

6.12. Requests for Multiple Accounts for the Same User

6.12.1. Requests for multiple user accounts for the same user must be accompanied by a business justification and the approval of a manager.

6.12.2. All Divisional or Program Security Analysts must save the documentation for all requests for multiple accounts for a period of 3 years, making it available to ISA upon request.

7. Implications

DES business units must review their existing rules and processes and immediately change them to suit this procedure.

8. Implementation Strategy

This procedure is effective for all DES business units as of its publication.

9. References

9.1. None

10. Attachments

10.1. None

11. Associated GITA IT Standards or Policies

11.1. None

12. Review Date

12.1. This document will be reviewed twelve (12) months from the original adoption date, and every twelve months thereafter.